

Notice of Allowability

Application No.

09/740,376

Applicant(s)

CHEN ET AL.

Examiner

Art Unit

Thomas M Ho

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 1/03/05.
2. ☒ The allowed claim(s) is/are 1.
3. ☒ The drawings filed on 7/30/01 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892) | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 6. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____. |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____ | 7. <input type="checkbox"/> Examiner's Amendment/Comment |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| | 9. <input type="checkbox"/> Other _____. |

Response to Arguments

Applicant's arguments, see pages 1-3, filed 10/25/04, with respect to Claim 1 have been fully considered and are persuasive. The rejection of 7/22/04 has been withdrawn.

Reasons for Allowance

Upon the initial reading of the subject matter found in claim 1, the Examiner noted marked similarities to the Montgomery Multiplication Method. Minor differences between applicant's function, and the Montgomery Multiplication Method were however found.

The Examiner initially rejected the comparing of the sum of the Z_i values with the sum of two products, the first product being the product of sums of the A_i and B_i terms, and the second product being the product of the sums of the N_i and Y_i terms.

In the previous rejection, the Examiner mapped the following claim elements with the prior art.


Comparing the sum of the Z_i values with the sum of two products, the first product being the product of the sums of the A_i and B_i terms, and the second product being the product of the sums of the N_i and Y_i terms, where the sum of the Z_i values (A of 14.36) are compared using the sums of two products($x_i y$ and $u_i m$) from 2.2 of 14.36.

Art Unit: 2134

Upon further examination though, it would appear that while a sum of the Z_i values is present (as A) and first and second products are present as shown in 2.2 of 14.36, and a comparison is present as shown in Item 3, this comparison is not with A against the sum of two products. Instead in the Montgomery Multiplication method, the comparison of A is performed against another value m.

While a seemingly small difference, the Examiner notes that in the cryptographic art dealing with mathematical functions, even small difference in equations can have drastically different mathematical implications and provide a new set of relationships.

For this reason, the rejection of 7/22/04 has been withdrawn.


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER